IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Janice M. Girouard, *et al.*	§	Group Art Unit: 2135
	§	
	§	Examiner: Shan, April Ying
Serial No.: 10/671,058	§	
	§	Atty Docket No.: AUS920030637US1
Filed: 09/25/2003	§	
	§	Customer No.: 34533
Title: Algorithmic Generation Of Passwords	§	
	§	Confirmation No.: 5828

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPEAL BRIEF

Honorable Commissioner:

This is an Appeal Brief filed pursuant to 37 CFR § 41.37 in response to the Final Office Action May 31, 2007 (hereinafter the "Office Action"), and pursuant to the Notice of Appeal filed August 30, 2007.

REAL PARTY IN INTEREST

The real party in interest in accordance with 37 CFR § 41.37(c)(1)(i) is the patent assignee, International Business Machines Corporation ("IBM"), a New York corporation having a place of business at Armonk, New York 10504.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences within the meaning of 37 CFR § 41.37(c)(1)(ii).

STATUS OF CLAIMS

Status of claims in accordance with 37 CFR § 41.37(c)(1)(iii): Twenty (20) claims are filed in the original application in this case. Claims 1-20 are rejected in the Office Action. Claims 1-20 are on appeal.

STATUS OF AMENDMENTS

Status of amendments in accordance with 37 CFR § 41.37(c)(1)(iv): No amendments were submitted after final rejection. The claims as currently presented are included in the Appendix of Claims that accompanies this Appeal Brief.

SUMMARY OF CLAIMED SUBJECT MATTER

Appellants provide the following concise summary of the claimed subject matter according to 37 CFR § 41.37(c)(1)(v). This summary includes a concise explanation of the subject matter defined in each of the independent claims involved in the appeal and includes references to the specification by page and line number and to the drawings by reference characters. The three independent claims involved in this appeal are claims 1, 8, and 15. Claims 1 is a method claim. Claim 8 is a system claim corresponding to the method of claim 1. Claim 15 is a computer program product claim corresponding to the method of claim 1. Claim 5, argued separately below, is method claim that depends from claim 1 and includes limitations in addition to those recited in claim 1.

Claim 1 recites a method for providing a password to an application (page 10, lines 22-23 and Figure 2). The method of claim 1 includes receiving, from a user, a passkey event

uniquely associated with one of a plurality of applications requiring a password (page 10, lines 23-26 and Figure 2, elements 202, 300, 210, 204A, and 204B). The method of claim 1 also includes receiving, from a user, a same master password for access to each of the plurality of applications (page 12, lines 14-15 and Figure 2, elements 208, 300, 204, 204A, and 204B). The method of claim 1 also includes applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password (page 13, lines 12-14 and Figure 2, elements 213, 212, 214, 210, 204, and 216). The method of claim 1 also includes submitting the application specific password to the application for access by the user (page 13, lines 25-26 and Figure 2, elements 218, 216, 204A, and 300).

Claim 8 recites a system for providing a password to an application (page 10, lines 22-23 and Figure 2). The system of claim 8 includes means for receiving, from a user, a passkey event uniquely associated with one of a plurality of applications requiring a password (page 10, lines 23-26 and Figure 2, elements 202, 300, 210, 204A, and 204B). The system of claim 8 also includes means for receiving, from a user, a same master password for access to each of the plurality of applications (page 12, lines 14-15 and Figure 2, elements 208, 300, 204, 204A, and 204B). The system of claim 8 also includes means for applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password (page 13, lines 12-14 and Figure 2, elements 213, 212, 214, 210, 204, and 216). The system of claim 8 also includes means for submitting the application specific password to the application for access by the user (page 13, lines 25-26 and Figure 2, elements 218, 216, 204A, and 300).

Claim 15 recites a computer program product for providing a password to an application (page 10, lines 22-23 and Figure 2). The computer program product of claim 15 includes a recording medium (page 7, lines 17-21). The computer program product of claim 15 also includes means, recorded on the recording medium, for receiving, from a user, a passkey event uniquely associated with one of a plurality of applications requiring a password (page 10, lines 23-26 and Figure 2, elements 202, 300, 210, 204A, and 204B). The computer program product of claim 15 also includes means, recorded on the

recording medium, for receiving, from a user, a same master password for access to each of the plurality of applications (page 12, lines 14-15 and Figure 2, elements 208, 300, 204, 204A, and 204B). The computer program product of claim 15 also includes means, recorded on the recording medium, for applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password (page 13, lines 12-14 and Figure 2, elements 213, 212, 214, 210, 204, and 216). The computer program product of claim 15 also includes means, recorded on the recording medium, for submitting the application specific password to the application for access by the user (page 13, lines 25-26 and Figure 2, elements 218, 216, 204A, and 300).

Claim 5 recites a method of applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password (page 16, lines 8-10, Figure 3, elements 212, 214, 210, 204, 216, 230, and 232). The method of claim 5 includes retrieving a character rule algorithm (page 16, lines 10-22, and Figure 3, elements 230, 232, and 250). The method of claim 5 also includes applying the character rule algorithm to the hashed character to generate a character rule compliant hashed character (page 16, line 24 – page 17, line 5 and Figure 3, elements 212, 214, 210, 204, 216, 234, 228, and 236).

GROUNDS OF REJECTION

In accordance with 37 CFR § 41.37(c)(1)(vi), Appellants provide the following concise statement for each ground of rejection:

1. Claims 1-3, 5-6, 8-10, 12-13, 15-17, and 19-20 are rejected under 35 U.S.C. § 102(e) as being anticipated by Henry, et al. (U.S. Patent No. 6,996,718).

2. Claims 4, 11, and 18 are rejected under 35 U.S.C. §103(a) as being obvious over Henry, et al. in view of Challener et al. (U.S. Patent No. 7,085,933).

3. Claims 7 and 14 are rejected under 35 U.S.C. §103(a) as being obvious over

Henry, et al. in view of D'Souza et al. (U.S. Patent No. 6,625,649).

ARGUMENT

Appellants present the following argument pursuant to 37 CFR § 41.37(c)(1)(vii) regarding the ground of rejection on appeal in the present case.

Argument Regarding The First Ground Of Rejection On Appeal: Claims 1-3, 5-6, 8-10, 12-13, 15-17, And 19-20 Are Rejected Under 35 U.S.C. § 102(e) As Being Anticipated By Henry, Et Al. (U.S. Patent No. 6,996,718)

Claims 1-3, 5-6, 8-10, 12-13, 15-17, and 19-20 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Henry. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). As explained in more detail below, Henry does not disclose each and every element of claim 1, and Henry therefore cannot be said to anticipate the claims of the present application within the meaning of 35 U.S.C. § 102(e).

Independent claim 1 recites:

> 1. A method for providing a password to an application, the method comprising:
>
> receiving, from a user, a passkey event uniquely associated with one of a plurality of applications requiring a password;
>
> receiving, from a user, a same master password for access to each of the plurality of applications;

applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password; and

submitting the application specific password to the application for access by the user.

Henry Does Not Disclose Receiving, From A User, A Passkey Event Uniquely Associated With One Of A Plurality Of Applications Requiring A Password

The Office Action takes the position that Henry at Figure 7 and column 4, lines 18-20, discloses the first element of claim 1: receiving, from a user, a passkey event uniquely associated with one of a plurality of applications requiring a password. Applicants respectfully note in response, however, that what Henry at Figure 7 in fact discloses is an exemplary user screen for a password transform calculator. The user screen includes a text field for inputting a user's account username and inputting a user's account location. In addition what Henry at column 4, lines 18-20, in fact discloses is:

> The user id and the server name cooperate to uniquely define a unique account belonging to the user.

That is, Henry at column 4, lines 18-20, discloses a user identification and server name cooperating to define a user account. Neither Henry's user screen for a password transform calculator nor Henry's user identification and server name cooperating to define a user account discloses receiving, from a user, a passkey event uniquely associated with one of a plurality of applications requiring a password as claimed in the present application. Henry does not disclose a passkey event as claimed here. A passkey event as defined in Applicants original specification at page 10, lines 26-27, is "an event received by an operating system that is created by a user's invoking a passkey." A passkey may be a designated key on a keyboard, buttons of a mouse, special hardware tokens, or any other input device. Henry does not disclose a passkey event that is created by a user's invoking such a passkey. Moreover, the passkey event as claimed here is

associated with one of a plurality of applications requiring a password. Henry does not disclose applications requiring a password but instead only discloses Web-based accounts requiring a password. Henry at column 1, lines 25-27, lists several examples of such Web-based accounts including "electronic commerce sites, primarily content based sites, electronic mail accounts, stock trading and/or research accounts, etc." Henry's Web-based accounts are not applications as claimed here and as such Henry does not disclose receiving, from a user, a passkey event uniquely associated with one of a plurality of applications requiring a password. Because Henry does not disclose each and every element and limitation of Applicants' claims, Henry does not anticipate Applicants' claims, and the rejections under 35 U.S.C. § 102(e) should be withdrawn.

Henry Does Not Disclose Applying A Hashing Algorithm Associated With The Passkey Event To The Master Password To Generate An Application Specific Password

The Office Action takes the position that Henry at the abstract, and column 3, line 60 – column 4, line 20, discloses the third element of claim 1: applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password. Applicants respectfully note in response, however, that what Henry at the abstract in fact discloses is:

> A common password method is disclosed which provides both convenience and security assurance for users who have multiple accounts protected by passwords. According to the present invention, a user only needs to remember a common password to access any of the user's accounts. A designated password for each account is generated by a hash function of the common password and some account-dependent information. The hash value is calculated at the user's computer, and then submitted as a designated password to a server. Thus, each account is protected by the distinct designated password, and the common password is never revealed in an unauthorized manner.

And what Henry at column 3, line 60 – column 4, line 20, in fact discloses is:

> In the present invention, to generate, process and validate the common password and associated designated passwords for each of a user's

> accounts, a password transform algorithm is utilized. In a preferred embodiment of the present invention, the password transform algorithm may be generalized as follows: Pd=Text(Hash(Ui+Pc+Si+Nr)) Where, Pd stands for a designated password, Ui for a user ID (such as a login ID selected by the user or provided by an account service provider), Pc for a common password (which is preferably selected by a user as discussed above), Si for a server name (such as the server name or URL of the user's account service provider), and Nr for a random number. The "Text( )" portion represents the text conversion and the "Hash( )" portion represents the hash function.
>
> The password transform algorithm is process in two major steps. The first step is to calculate a hash function ("Hash ( )") by taking the common password and some account-dependent information. Any hash functions as known in the art, such as SHA [SHA] and MD5 [MD5], could serve this purpose. The account-dependent information includes a user ID, a server name that indicates the account location, and a random number that is associated with the account and stored at the server. The should be readily available and need not be specifically remembered by the user. The user id and the server name cooperate to uniquely define a unique account belonging to the user.

That is, Henry at the abstract and column 3, line 60 – column 4, line 20, discloses a designated password generated by a hash function and some account-dependent information. Henry's designated password generated by a hash function and some account-dependent information does not disclose applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password as claimed in the present application. The hashing algorithm as claimed in the present application is associated with a passkey event. Henry does not disclose, however, at this reference point, or anywhere else in Henry, a passkey event as claimed in the present application and, as such, Henry cannot disclose a hashing algorithm associated with such a passkey event. Henry does not disclose therefore applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password as claimed in the present application. Because Henry does not disclose each and every element and limitation of Applicants' claims, Henry does not anticipate Applicants' claims, and the rejections under 35 U.S.C. § 102(e) should be withdrawn.

Relations Among Claims

Independent claims 8 and 15 are system and computer program product claims for providing a password to an application corresponding to independent method claim 1 that include "means for" and "means, recorded on [a] recording medium, for:" providing a password to an application. As explained above in detail, Henry does not disclose a method for providing a password to an application. Therefore, for the same reasons that Henry does not disclose a method for providing a password to an application, Henry also does not disclose systems and computer program products for providing a password to an application corresponding to independent claims 8 and 15. Independent claims 8 and 15 are therefore patentable and should be allowed.

Claims 2-7, 9-14, and 16-20 depend respectively from independent claims 1, 8, and 15. Each dependent claim includes all of the limitations of the independent claim from which it depends. Because Henry does not disclose each and every element of the independent claims, Henry does not disclose each and every element of the dependent claims of the present application. As such, claims 2-7, 9-14, and 16-20 are also patentable and should be allowed.

In addition to the fact that Henry does not disclose elements from the independent claims that are included in the dependent claims, there is another reason that Henry does not anticipate the dependent claims of the present application – that is, Henry itself does not disclose the elements of the dependent claims that Henry is purported to disclose according to the Office Action. Consider the second element of dependent claim 5 as an example. The Office Action takes the position that Henry at column 3, line 66 - column 4, line 31, discloses the second element of claim 5: applying the character rule algorithm to the hashed character to generate a character rule compliant hashed character. What Henry at column 3, line 66 - column 4, line 31 in fact discloses is a password transform algorithm that includes a hash function and a text conversion function. Henry's password transform algorithm does not disclose the second element of claim 5 of the present

application because Henry's password transform algorithm is not a character rule algorithm used to generate a character rule compliant hashed character. For precisely similar reasons, Henry does not disclose any of the other elements of the dependent claims in the present application. Because Henry does not disclose each and every element and limitation of the dependent claims of the present application Henry does not anticipate the dependent claims and the rejections under 35 U.S.C. § 103(a) should be withdrawn.

Argument Regarding The Second Ground Of Rejection On Appeal: Claims 4, 11, And 18 Are Rejected Under 35 U.S.C. §103(a) As Being Obvious Over Henry, Et Al. In View Of Challener Et Al. (U.S. Patent No. 7,085,933)

Claims 4, 11, and 18 stand rejected for obviousness under 35 U.S.C. § 103(a) as being unpatentable over Henry in view of Challener. To establish a prima facie case of obviousness, the proposed combination of the references must teach or suggest all of the claim limitations of dependent claims 4, 11, and 18. *In re Royka*, 490 F.2d 981, 985, 180 USPQ 580, 583 (CCPA 1974). Dependent claims 4, 11, and 18 depend from independent claims 1, 8, and 15 and include all the limitations of the independent claims from which they depend. In rejecting dependent claims 4, 11, and 18, the Office Action relies on Henry as disclosing each and every element of independent claims 1, 8, and 15. As shown above, Henry in fact does not disclose each and every element of independent claims 1, 8, and 15. Because Henry does not disclose each and every element of independent claims 1, 8, and 15, the combination of Henry and Challener cannot possibly disclose each and every element of dependent claims 4, 11, and 18. The proposed combination of Henry and Challener, therefore, cannot establish a prima facie case of obviousness, and the rejections under 35 U.S.C. § 103(a) should be withdrawn.

Argument Regarding The Second Ground Of Rejection On Appeal: Claims 7 And 14 Are Rejected Under 35 U.S.C. §103(a) As Being Obvious Over Henry, Et Al. In View Of D'Souza Et Al. (U.S. Patent No. 6,625,649)

Claims 7 and 14 stand rejected for obviousness under 35 U.S.C. § 103(a) as being unpatentable over Henry in view of D'Souza. To establish a prima facie case of

obviousness, the proposed combination of the references must teach or suggest all of the claim limitations of dependent claims 7 and 14. *In re Royka*, 490 F.2d 981, 985, 180 USPQ 580, 583 (CCPA 1974). Dependent claims 7 and 14 depend from independent claims 1 and 8 and include all the limitations of the independent claims from which they depend. In rejecting dependent claims 7 and 14, the Office Action relies on Henry as disclosing each and every element of independent claims 1 and 8. As shown above, Henry in fact does not disclose each and every element of independent claims 1 and 8. Because Henry does not disclose each and every element of independent claims 1 and 8, the combination of Henry and D'Souza cannot possibly disclose each and every element of dependent claims 7 and 14. The proposed combination of Henry and D'Souza, therefore, cannot establish a prima facie case of obviousness, and the rejections under 35 U.S.C. § 103(a) should be withdrawn.

CONCLUSION OF APPELLANT'S ARGUMENTS

Claims 1-3, 5-6, 8-10, 12-13, 15-17, and 19-20 stand rejected under 35 U.S.C. § 102 as being anticipated by Henry. Henry does not disclose each and every element of Applicants' claims. Henry therefore does not anticipate Applicants' claims. Claims 1-3, 5-6, 8-10, 12-13, 15-17, and 19-20 are therefore patentable and should be allowed. Applicants respectfully request reconsideration of claims 1-3, 5-6, 8-10, 12-13, 15-17, and 19-20.

Claims 4, 11, and 18 stand rejected under 35 U.S.C. § 103 as obvious over Henry in view of Challener. The combination of Henry and Challener does not teach or suggest each and every element of Applicants' claims. Claims 4, 11, and 18 are therefore patentable and should be allowed. Applicants respectfully request reconsideration of claims 4, 11, and 18.

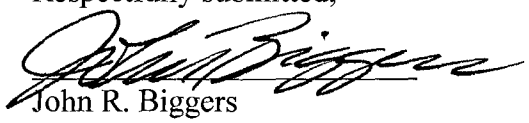
Claims 7 and 14 stand rejected under 35 U.S.C. § 103 as obvious over Henry in view of D'Souza. The combination of Henry and D'Souza does not teach or suggest each and

every element of Applicants' claims. Claims 7 and 14 are therefore patentable and should be allowed. Applicants respectfully request reconsideration of claims 7 and 14.

In view of the arguments above, reversal on all grounds of rejection is requested.

The Commissioner is hereby authorized to charge or credit Deposit Account No. 09-0447 for any fees required or overpaid.

Respectfully submitted,

Date: October 30, 2007 By: 

John R. Biggers
Reg. No. 44,537
Biggers & Ohanian, LLP
P.O. Box 1469
Austin, Texas 78767-1469
Tel. (512) 472-9881
Fax (512) 472-9887
ATTORNEY FOR APPELLANTS

APPENDIX OF CLAIMS ON APPEAL IN PATENT APPLICATION OF JANICE M. GIROUARD, ET AL., SERIAL NO. 10/671,058

CLAIMS

Listing of claims:

1. A method for providing a password to an application, the method comprising:

receiving, from a user, a passkey event uniquely associated with one of a plurality of applications requiring a password;

receiving, from a user, a same master password for access to each of the plurality of applications;

applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password; and

submitting the application specific password to the application for access by the user.

2. The method of claim 1 wherein applying a hashing algorithm associated with the passkey event to the same master password to generate an application specific password comprises:

retrieving a hash value associated with the passkey event; and

applying the hash value to at least one character of the same master password to generate at least one hashed character.

3. The method of claim 2 wherein retrieving a hash value associated with the passkey event comprises retrieving hash value from a user's configuration file.

4. The method of claim 2 wherein retrieving a hash value associated with the passkey event comprises retrieving a hash value from a configuration register.

5. The method of claim 2 wherein applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password comprises:

retrieving a character rule algorithm; and

applying the character rule algorithm to the hashed character to generate a character rule compliant hashed character.

6. The method of claim 3 wherein applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password comprises:

retrieving a master rule algorithm; and

applying the master rule algorithm.

7. The method of claim 1, wherein receiving, from a user, a passkey event uniquely associated with any given one of the plurality of applications comprises receiving, from a user, an event created by a user's engaging a keyboard key.

8. A system for providing a password to an application, the system comprising:

means for receiving, from a user, a passkey event uniquely associated with one of a plurality of applications requiring a password;

means for receiving, from a user, a same master password for access to each of the plurality of applications;

means for applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password; and

means for submitting the application specific password to the application for access by the user.

9. The system of claim 8 wherein means for applying a hashing algorithm associated with the passkey event to the same master password to generate an application specific password comprises:

means for retrieving a hash value associated with the passkey event; and

means for applying the hash value to at least one character of the same master password to generate at least one hashed character.

10. The system of claim 9 wherein means for retrieving a hash value associated with the passkey event comprises means for retrieving hash value from a user's configuration file.

11. The system of claim 9 wherein means for retrieving a hash value associated with the passkey event means for comprises retrieving a hash value from a configuration register.

12. The system of claim 9 wherein means for applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password comprises:

means for retrieving a character rule algorithm; and

means for applying the character rule algorithm to the hashed character to generate a character rule compliant hashed character.

13. The system of claim 10 wherein means for applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password comprises:

means for retrieving a master rule algorithm; and

means for applying the master rule algorithm.

14. The system of claim 8, wherein means for receiving, from a user, a passkey event uniquely associated with any given one of the plurality of applications comprises means for receiving, from a user, an event created by a user's engaging a keyboard key.

15. A computer program product for providing a password to an application, the computer program product comprising:

a recording medium;

means, recorded on the recording medium, for receiving, from a user, a passkey event uniquely associated with one of a plurality of applications requiring a password;

means, recorded on the recording medium, for receiving, from a user, a same master password for access to each of the plurality of applications;

means, recorded on the recording medium, for applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password; and

means, recorded on the recording medium, for submitting the application specific password to the application for access by the user.

16. The computer program product of claim 15 wherein means, recorded on the recording medium, for applying a hashing algorithm associated with the passkey event to the same master password to generate an application specific password comprises:

means, recorded on the recording medium, for retrieving a hash value associated with the passkey event; and

means, recorded on the recording medium, for applying the hash value to at least one character of the same master password to generate at least one hashed character.

17. The computer program product of claim 16 wherein means, recorded on the recording medium, for retrieving a hash value associated with the passkey event comprises means, recorded on the recording medium, for retrieving hash value from a user's configuration file.

18. The computer program product of claim 16 wherein means, recorded on the recording medium, for retrieving a hash value associated with the

passkey event means, recorded on the recording medium, for comprises retrieving a hash value from a configuration register.

19. The computer program product of claim 16 wherein means, recorded on the recording medium, for applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password comprises:

means, recorded on the recording medium, for retrieving a character rule algorithm; and

means, recorded on the recording medium, for applying the character rule algorithm to the hashed character to generate a character rule compliant hashed character.

20. The computer program product of claim 17 wherein means, recorded on the recording medium, for applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password comprises:

means, recorded on the recording medium, for retrieving a master rule algorithm; and

means, recorded on the recording medium, for applying the master rule algorithm.

APPENDIX OF EVIDENCE ON APPEAL IN PATENT APPLICATION OF JANICE M. GIROUARD, ET AL., SERIAL NO. 10/671,058

This is an evidence appendix in accordance with 37 CFR § 41.37(c)(1)(ix).

There is in this case no evidence submitted pursuant to 37 CFR §§ 1.130, 1.131, or 1.132, nor is there in this case any other evidence entered by the examiner and relied upon by the Appellants.

RELATED PROCEEDINGS APPENDIX

This is a related proceedings appendix in accordance with 37 CFR § 41.37(c)(1)(x). There are no decisions rendered by a court or the Board in any proceeding identified pursuant to 37 CFR § 41.37(c)(1)(ii).